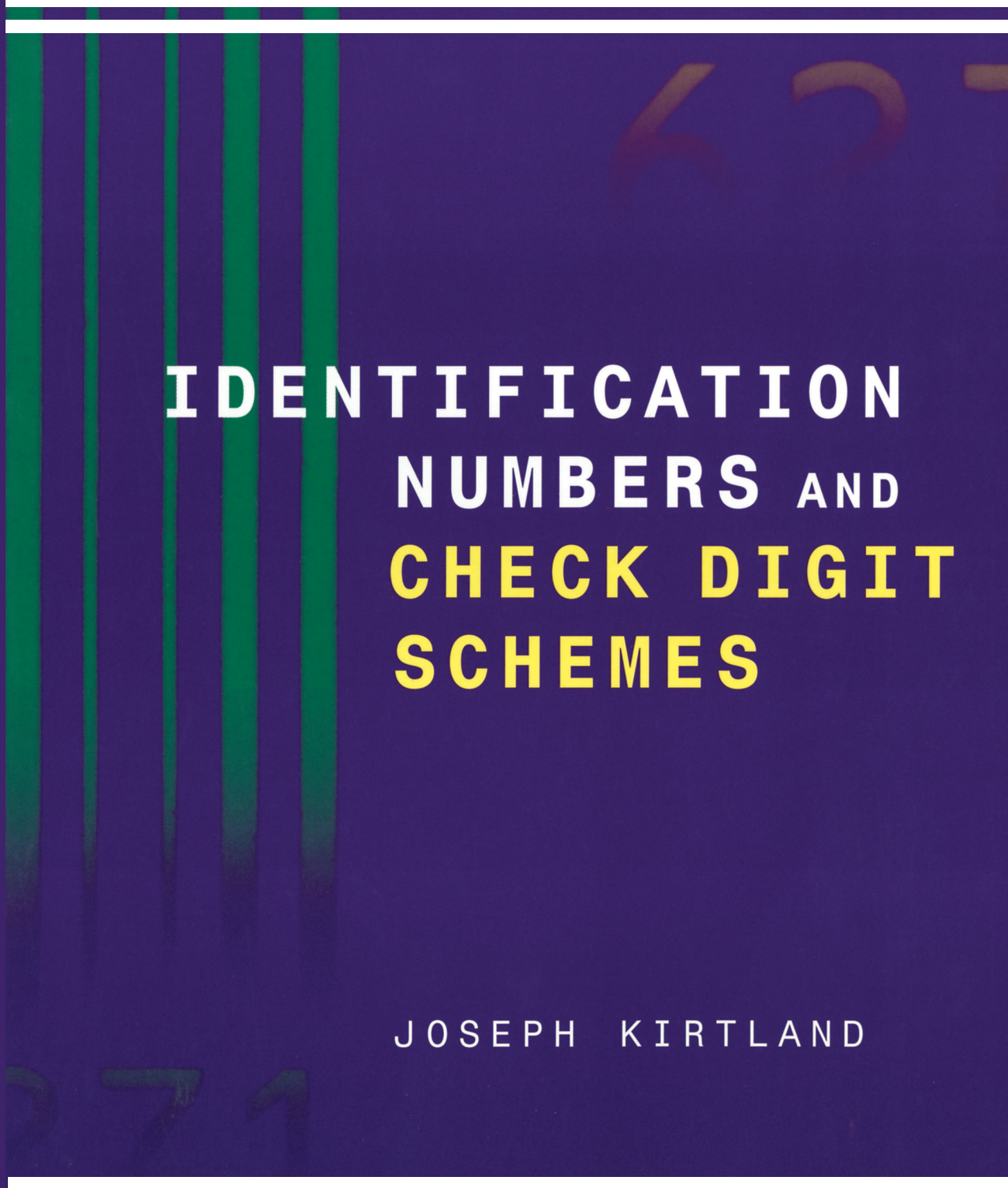
AMS / MAA | CLASSROOM RESOURCE MATERIALS VOL 18



IDENTIFICATION NUMBERS AND CHECK DIGIT SCHEMES

JOSEPH KIRTLAND

MAA PRESS
An Imprint of the AMERICAN MATHEMATICAL SOCIETY

Identification Numbers and Check Digit Schemes

This material is based upon work supported by the
National Science Foundation under grant number DUE-9752632

This project was supported, in part,
by the
National Science Foundation
Opinions expressed are those of the authors
and not necessarily those of the foundation

Library of Congress Number 00-108052

ISBN 10: 0-88385-720-0
ISBN 13: 978-0-88385-720-5

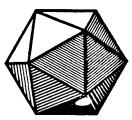
Printed in the United States of America

Current Printing:
10 9 8 7 6 5 4 3 2

10.1090/clrm/018

Identification Numbers and Check Digit Schemes

Joseph Kirtland
Marist College



Published and distributed by
The Mathematical Association of America

CLASSROOM RESOURCE MATERIALS

This series provides supplementary material for students and their teachers—laboratory exercises, projects, historical information, textbooks with unusual approaches for presenting mathematical ideas, career information, and much more.

101 Careers in Mathematics, edited by Andrew Sterrett

Archimedes: What Did He Do Besides Cry Eureka?, Sherman Stein

Calculus Mysteries and Thrillers, R. Grant Woods

Combinatorics: A Problem Oriented Approach, Daniel A. Marcus

A Course in Mathematical Modeling, Douglas Mooney and Randall Swift

Cryptological Mathematics, Robert Edward Lewand

Elementary Mathematical Models, Dan Kalman

Geometry From Africa: Mathematical and Educational Explorations, Paulus Gerdes

Identification Numbers and Check Digit Schemes, Joseph Kirtland

Interdisciplinary Lively Application Projects, edited by Chris Arney

Laboratory Experiences in Group Theory, Ellen Maycock Parker

Learn from the Masters, Frank Swetz, John Fauvel, Otto Bekken, Bengt Johansson, and Victor Katz

Mathematical Modeling in the Environment, Charles Hadlock

A Primer of Abstract Mathematics, Robert B. Ash

Proofs Without Words, Roger B. Nelsen

Proofs Without Words II, Roger B. Nelsen

A Radical Approach to Real Analysis, David M. Bressoud

She Does Math!, edited by Marla Parker

MAA Service Center
P.O. Box 91112
Washington, DC 20090-1112
1-800-331-1MAA FAX: 1-301-206-9789

Acknowledgement

Many people made this book possible, and I thank them all. First, I am extremely grateful to Pau-San Haruta of the Marist College English Department for her tireless efforts and valuable insights in the course of this project. Second, I thank Joe Gallian of the University of Minnesota–Duluth, whose numerous articles motivated this book and whose proofreading helped hone it. I also thank Louis Gross, Dorothy Buerk, and Kay Losey, whose constructive comments were greatly appreciated. Finally, I owe a great deal to April Sullivan, Marist College class of 1999, and Christina Sheedy, Marist College class of 2000, each of whom spent a summer helping me gather information. This book would not have been possible without them.

To my wife Cindy, son Timmy, and daughter Betsy.

Contents

Introduction

0.1 To the Student

The ability to store, retrieve, and transmit data accurately is a central aspect of today's society. To make this process work efficiently, *identification numbers* are used to represent or encode information pertaining to products, documents, accounts, or individuals. One such system in place today generates a Universal Product Code (UPC) for every item sold in a grocery store. A UPC identifies not only the specific product but also the type of product and its manufacturer. This gives grocery stores a convenient and effective way to maintain inventory and keep track of sales (each store associates a price with the UPC that appears on the cash register when the product's bar code is scanned at the checkout counter). Numbers are also used to identify books (International Standard Book Numbers or ISBNs), individuals (social security numbers), library holdings, bank accounts, UPS packages, drivers' licenses, credit cards, and much more.

Given that identification numbers provide a convenient way to transmit information easily and accurately, they are recorded onto documents, typed or scanned into computers, sent via the Internet, or transmitted in some other fashion millions of times a day. Banks routinely transfer money electronically by using routing and account numbers, and consumers frequently complete sales with credit card numbers. Since these types of transactions occur so frequently, errors are bound to happen. For example, the number 12345 could be transmitted and incorrectly recorded as 12346 or as 12354. A bank would not want to transfer money into the wrong bank account, and consumers and retailers do not want charges billed to the wrong credit card account.

With our heavy reliance on identification numbers to transmit information and the likelihood that sooner or later a transmission error will occur, it is crucial to know when an identification number has been transmitted incorrectly. Specifically, the receiver of that number must have a way to determine whether the number received is incorrect. If no verification system has been established, the only way of knowing is to contact the sender. But contacting the sender is not always possible or feasible, and it may be time consuming. This difficulty has motivated the creation of methods that the receiver

can use, independent of the sender, to recognize when an identification number has been transmitted incorrectly. The goal of this book is to present the mathematical methods, called *check digit schemes*, that do this.

Identification numbers, and the check digit schemes that detect when these numbers have been transmitted incorrectly, are crucial for the quick storage, retrieval, and transfer of vast amounts of information. In this book, a variety of check digit schemes are discussed. Check digit schemes vary in their ability to catch errors. Some, such as the airline ticket scheme, do not catch every occurrence of the most common type of error, while others, such as the ISBN scheme, catch most error patterns. Consequently, criteria for judging the reliability of check digit schemes are a central concern of this book.

0.2 To the Professor

This text is ideal for a liberal arts mathematics class. The book is organized to allow students to move from simple mathematical concepts and check digit schemes to more complex ideas. Not only are all mathematical concepts developed within the context of studying check digit schemes, but as each mathematical topic is studied, other applications are discussed. This will lead to a study of not only check digit schemes, but also "public key" cryptography systems, graphing data, presenting data, and symmetry.

Chapter 1 discusses a variety of identification number systems and establishes the mathematical terminology that will be used to study check digit schemes. In addition, the criteria used to determine the dependability of a scheme are presented.

Chapter 2 begins with a presentation of basic properties of integers and an introduction to modulo arithmetic. The concepts developed are then applied to an investigation of the check digit schemes used for United States' postal money orders, airline tickets, UPCs, and ISBNs. The reliability of each scheme is a central aspect of this discussion. Finding methods that address shortcomings of these schemes motivates the material covered in the remaining chapters. The same number-theoretic concepts are also applied to a discussion of cryptography, the art of sending secret messages. Special attention is paid to the RSA "public key" cryptography system, which is used to send sensitive data over the Internet.

In Chapter 3, sets, functions, and permutations are considered. These concepts play a role in the construction of more advanced check digit schemes and are central to *hashing functions*. A hashing function is the process used to take information and represent it as an identification number. The check digit scheme developed by IBM is also presented. In addition, the use of graphs to present and study functions and data is discussed.

The discussion in Chapter 4 is focused on symmetry and rigid motions. The notation established in Chapter 3 for permutations is used in a mathematical investigation of the symmetries of a variety of different shapes. The symmetries of a pentagon form the basis of the very reliable Verhoeff check digit scheme presented in Chapter 5. Furthermore, the use of rigid motions to create elaborate patterns will serve as an introduction to the discussion of group theory that begins Chapter 5.

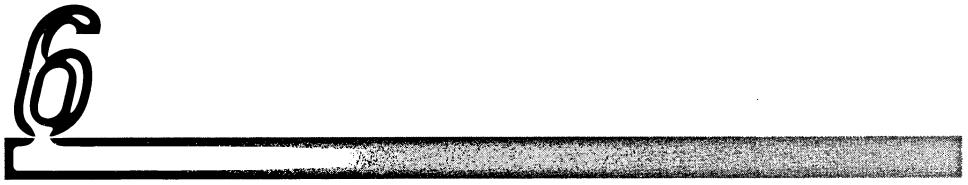
In Chapter 5, an introduction to the fundamentals of group theory is presented. The

concepts discussed, along with those presented in the previous chapters, culminate in the Verhoeff check digit scheme, the most sophisticated and reliable scheme considered in the book. The check digit scheme used with German money, which is based on the Verhoeff scheme, is also considered.

Along with the mathematical content described above, this book provides writing and group activities. These activities can be integrated into a student-centered approach. At the beginning of each section is a preliminary activity that has the students exploring and working with the concepts to be introduced. The notions that the students develop are then cultivated in that section. At the end of the section, traditional exercises, group activities, and writing assignments are given for further exploration.

Integral to this approach is the use of writing to develop and present mathematical understanding (see [17] and [24] for more information on the use of writing in the teaching of mathematics). Writing is not only a way to express mathematical understanding, but a way to develop that understanding. As each mathematical topic is investigated, the students use writing to improve and communicate their understanding of that topic and how it is applied. Students should write at the beginning, middle, and end of the learning process. The preliminary activities have them writing to investigate. This work is then rewritten or used to complete homework exercises and group activities, which are, in turn, used to complete larger writing assignments or essays. Through this writing and rewriting process, students gain a deeper understanding of mathematics and its diverse applications.

Writing to develop mathematical understanding will also improve communication skills. Many of the components of the mathematical process are rhetorical modes or critical writing strategies. Defining, serializing, classifying, comparing, generalizing, analyzing, and arguing are skills crucial to mathematics, but each is also a strategy that must be mastered to become an effective writer. Writing and paper assignments are included to help students develop each of these strategies.



Bibliography

Armstrong, M. A. *Groups and Symmetry.* Springer-Verlag, New York City, 1988.

Beker, H., and Piper, F. *Cipher Systems: The Protection of Communications.* Wiley, New York City, 1982.

Bernard, K. J., and Wellenzohn, H. J. *Foundations of Mathematics.* H&H Publishing Company, Clearwater, FL, 1997.

Beutelspacher, A. *Cryptology.* The Mathematical Association of America, Washington, D.C., 1994.

Boneh, D., Twenty Years of Attacks on the RSA Cryptosystem. *Notices of the AMS,* 46(2), 1999, 203–213.

Briggs, J. *Fractals: The Patterns of Chaos.* Simon and Schuster, New York City, 1992.

Burton, D. M. *Elementary Number Theory.* McGraw Hill, New York City, 1998.

Burton, D. M. *The History of Mathematics.* WCB McGraw Hill, Boston, 1999.

D'Angelo, J. P., and West, D. W. *Mathematical Thinking: Problem Solving and Proofs.* Prentice Hall, Upper Saddle River, NJ, 1997.

Davis, D. *The Nature and Power of Mathematics.* Princeton University Press, Princeton, NJ, 1993.

Devlin, K., *Mathematics, The Science of Patterns: The Search for Order in Life, Mind, and the Universe.* W.H. Freeman, New York City, 1994.

Dubinsky, E., and Harvel, G., eds. *The Concept of Function: Aspects of Epistemology and Pedagogy.* MAA Notes, No. 25. The Mathematical Association of America, Washington, D.C., 1992.

Escher, M. C. *The Infinite World of M. C. Escher.* Abradale Press, New York City, 1984.

Escher, M. C. *Escher on Escher.* H.N. Abrams, New York City, 1989.

Field, M., and Golubitsky, M. *Symmetry in Chaos: A Search for Pattern in Mathematics, Art, and Nature.* Oxford University Press, Oxford, 1995.

Gallian, J. A. *Contemporary Abstract Algebra.* Houghton Mifflin, Boston, 1998.

Garlièнski, J. *The Enigma War.* Scribner, New York City, 1979.

Gardner, M. *Time Travel and Other Mathematical Bewilderments.* W.H. Freeman, New York City, 1988.

Gardner, M. *The New Ambidestrous Universe: Symmetry and Asymmetry from Mirror Reflections to Superstrings.* W.H. Freeman, New York City, 1990.

Grünbaum, B., *Tilings and Patterns.* Freeman, New York City, 1987.

Halmos, P. R. *Naive Set Theory.* Springer-Verlag, New York City, 1974.

Hannabuss, K. Sound and Symmetry. *The Mathematical Intelligencer*, 19(4), 1997, 16–21.

Hargittai, I., ed. *Symmetry: Unifying Human Understanding.* Pergamon, New York City, 1986.

Harris, R. The Power of Information Graphics. *IIE Solutions*, 31, 1999, 26–27.

Herstein, I. N. *Abstract Algebra.* Prentice Hall, Upper Saddle River, NJ, 1990.

Humphreys, J. F. *Numbers, Groups, and Codes.* Cambridge University Press, Cambridge, 1989.

Humphreys, J. F. *A Course in Group Theory.* Oxford University Press, New York City, 1997.

Isihara, P., and Knapp, M. Basic Z_{12} Analysis of Musical Chords. *UMAP Journal*, 14(4), 1993, 319–348.

Johnston, B. L., and Richman, R. *Numbers and Symmetry: An Introduction to Algebra.* CRC Press, Boca Raton, 1997.

Jones, C. *Navajo Code Talkers: Native American Heroes.* Tudor Publishers, Greensboro, 1997.

Kawano, K., et al. *Warriors: Navajo Code Talkers.* Northland Publishing, Flagstaff, 1990.

Khan, D. *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939–1943.* Houghton Mifflin, Boston, 1991.

Kahn, D. *The Codebreakers: The Comprehensive History of Secret Communications from Ancient Times to the Internet.* Scribner, New York City, 1996.

Lee, B. *Marching Orders: The Untold Story of World War II.* Crown Publishers, New York City, 1995.

Lewin, R. *The American Magic: Codes, Ciphers, and the Defeat of Japan.* Farrar Straus Giroux, New York City, 1982.

Luciano, D., and Prichett, G. Cryptology: From Caesar Ciphers to Public-Key Cryptosystems. *College Mathematics Journal*, 18(1), 1987, 2–17.

Menezes, A. J., van Oorschot, P., and Vanstone, S. *Handbook of Applied Cryptography.* CRC Press, Boca Raton, 1996.

Mueller, A., et al. More Missouri Breaks. *UMAP Journal*, 13(4), 1992, 351–352.

Newton, D. E. *Encyclopedia of Cryptology.* ABC-CLIO, Santa Barbara, 1997.

Ogilvy C. S., and Anderson, J. T. *Excursions in Number Theory.* Dover, New York City, 1966.

Ore, O. *Invitation to Number Theory.* Random House, New York City, 1967.

Pedersen, F. D. *Modern Algebra: A Conceptual Approach.* W.C. Brown, Dubuque, Iowa, 1993.

Pinter, C. C. *A Book of Abstract Algebra.* McGraw Hill, New York City, 1990.

Pless, V., *Introduction to the Theory of Error-Correcting Codes.* Wiley, New York City, 1982.

Pomerance, C. The Search for Prime Numbers. *Scientific American*, 247, 1982, 122–130.

Prados, J. *Combined Fleet Decoded: The Secret History of American Intelligence and the Japanese Navy in World War II.* Random House, New York City, 1995.

Richardson, D., and St. John, P. Plotting to Succeed. *Geographical Magazine*, 64(12), 1992, 42–44.

Roberts, J. *Lure of the Integers.* The Mathematical Association of America, Washington, D.C., 1992.

Schattschneider, D. *Visions of Symmetry: Notebooks, Periodic Drawings, and Related Work of M. C. Escher.* W. H. Freeman, New York City, 1990.

Seberry, J., and Pieprzyk, J. *Cryptography: An Introduction to Computer Security.* Prentice Hall, Upper Saddle River, NJ, 1989.

Stewart, I. The Art of Elegant Tiling. *Scientific American*, 281(1), 1999, 96–98.

Stinson, D. R., *Cryptography: Theory and Practice.* CRC Press, Boca Raton, 1995.

UPC Symbol Specification Manual. Uniform Code Council, Dayton, Ohio, 1986.

Vinzant, C. What Hidden Meanings Are Embedded in Your Social Security Number? *Fortune*, 139, 1999, 32.

Welchman, G. *The Hut Six Story: Breaking the Enigma Codes.* McGraw Hill, New York City, 1982.

Wertenbaker, C. Nature's Patterns. *Parabola*, 24 1999, 5–12.

White, A. T. Fabian Stedman: The First Group Theorist? *American Mathematical Monthly*, 103(9), 1996, 771–778.

Wood, E. F. Self-Checking Codes: An Application of Modular Arithmetic. *Mathematics Teacher*, 80, 1987, 312–316.

Wrixon, F. B. *Codes and Ciphers.* Prentice Hall, Upper Saddle River, NJ, 1992.

Wussing, H. *The Genesis of the Abstract Group Concept.* MIT Press, Cambridge, 1984.

Zimmermann, R. R. Cryptography for the Internet. *Scientific American*, 279(4), 1998, 110–115.

References Cited

[1] Brown, D. A. H., Construction of Error Detection and Error Correction Codes to Any Base. *Electronic Letters*, 9, 1973, 290.

[2] Durbin, J .R., *Modern Algebra: An Introduction.* Wiley, New York City, 1992.

[3] Gallian, J. A., Check Digit Methods. *International Journal of Applied Engineering Education*, 5(4), 1989, 503–505.

[4] Gallian, J. A., The Mathematics of Identification Numbers. *College Mathematics Journal*, 22(3), 1991, 194–202.

[5] Gallian, J. A., Assigning Driver's License Numbers. *Mathematics Magazine*, 64(1), 1991, 13–22.

[6] Gallian, J. A., Error Detection Methods. *ACM Computing Surveys*, 28(3), 1996, 504–517.

[7] Gallian, J. A., and Winters, S., Modular Arithmetic in the Marketplace. *American Mathematical Monthly*, 95, 1988, 548–551.

[8] Garlìenski, J., *The Enigma War.* Scribner, New York City, 1979.

[9] Grätzer, G., *Math into Latex: An Introduction to Latex and AMS-Latex.* Birkhäuser, Boston, 1996.

[10] Gumm, H. P., A New Class of Check-Digit Methods for Arbitrary Number Systems. *IEEE Transactions on Information*, 31, 1985, 102–105.

[11] Gumm, H. P., Encoding of Numbers to Detect Typing Errors. *International Journal of Applied Engineering Education*, 2, 1986, 61–65.

[12] *The ISBN System Users' Manual.* International ISBN Agency, Berlin, 1986.

[13] Khan, D., *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939–1943.* Houghton Mifflin, Boston, 1991.

[14] Koblitz, N., *A Course in Number Theory and Cryptography.* Springer-Verlag, New York City, 1987.

[15] Lay, D. C., *Linear Algebra and Its Applications.* Addison-Wesley, Reading, Mass., 1994.

[16] Lewin, R., *The American Magic: Codes, Ciphers, and the Defeat of Japan.* Farrar Straus Giroux, New York City, 1982.

[17] Meier, J., and Rishell, T., *Writing in the Teaching and Learning of Mathematics.* The Mathematical Association of America, Washington, D.C., 1998.

[18] Prados, J., *Combined Fleet Decoded: The Secret History of American Intelligence and the Japanese Navy in World War II.* Random House, New York City, 1995.

[19] Rivest, R. L., Shamir, A., and Adleman, L., *A Method for Obtaining Digital Signatures and Public-Key Crypotosystems.* Laboratory for Computer Science, M.I.T., LCS/TM-82 (April 1977).

[20] Rivest, R. L., Shamir, A., and Adleman, L., A Method for Obtaining Digital Signatures and Public-Key Crypotosystems. *Communications of the ACM*, 21(2), 1978, 120–126.

[21] Schay, G., *Introduction to Linear Algebra.* Jones and Bartlett Publishers, Sudbury, Mass., 1997.

[22] Sethi, A. S., Rajaraman, V., and Kenjale. P. S., An Error Correcting Scheme for Alphanumeric Data. *Information Processing Letters*, 7, 1978, 72–77.

[23] Sinkov, A. *Elementary Cryptoanalysis: A Mathematical Approach.* Random House, New York City, 1968.

[24] Sterrett, A., ed., *Using Writing to Teach Mathematics.* MAA Notes no. 16, The Mathematical Association of America, Washington, D.C., 1990.

[25] Tuchinsky, P. M., International Standard Book Numbers. *UMAP Journal*, 5, 1989, 41–54.

[26] Verhoeff, J., *Error Detecting Decimal Codes.* Mathematical Centre, Amsterdam, 1969.

[27] Welchman, G., *The Hut Six Story: Breaking the Enigma Codes.* McGraw Hill, New York City, 1982.

[28] Welsh, D., *Codes and Cryptography.* Oxford University Press, New York City, 1988.

[29] Winters, S. J., Error Detecting Schemes Using Dihedral Groups. *UMAP Journal*, 11, 1990, 299–308.

INDEX

Identification numbers, used to encode information pertaining to products, documents, accounts, or individuals, are recorded onto documents, typed or scanned into computers, sent via the Internet, or transmitted in some other fashion millions of times a day. Given the heavy reliance on these numbers to transmit information and the possibility that a transmission error may occur, many add an extra digit or check digit that is used to determine if the identification number has been transmitted incorrectly. The mathematical process, called a check digit scheme, is used by the receiver of the number, independent of the sender, to recognize when a transmission error has occurred. This book presents the mathematics behind a variety of check digit schemes used today. Special attention is given to the airline ticket, United States Post Office money order, UPC, ISBN, IBM and Verhoeff schemes. Topics from number theory, set theory, and group theory are not only used to develop the schemes presented, but are used to develop topics from cryptography (RSA) and symmetry.

It may come as a surprise, but check digit schemes vary in their ability to catch errors. Some such as the airline ticket scheme, do not catch every occurrence of the most common type of error, while others, such as the ISBN scheme, catch most error patterns. Consequently, the criteria used to judge the reliability of a scheme is a central theme of this book.

This book will be of interest to a wide audience, especially those interested in mathematics at work. It is an ideal text for a liberal arts mathematics class. The book is organized to allow students to move from simple mathematical concepts and check digit schemes to more complex ideas. It also provides writing and group activities, which can be integrated into a student-centered approach.

Joseph Kirtland received his Ph.D. in mathematics from the University of New Hampshire. His main mathematical interest is finite group theory, and he has published a number of articles in the area of both finite and infinite group theory. Professor Kirtland joined the faculty at Marist College in 1992. A highly respected teacher, he has been selected six times by students for the Faculty Recognition Award in the School of Computer Science and Mathematics. In the fall of 2000, he was presented with the Board of Trustee's Distinguished Teaching Award. He has been active in the Metropolitan New York section of the Mathematical Association of America. He and his wife Cindy have two children, Timmy and Betsy.